

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

TYSON LIAU *and* RICHARD TENG, *on behalf of
themselves and on behalf of others similarly situated,*

Plaintiffs,

-v-

WEEE! INC.,

Defendant.

23 Civ. 1177 (PAE)

OPINION & ORDER

PAUL A. ENGELMAYER, District Judge:

Plaintiffs Tyson Liao and Richard Teng are former customers of defendant Weee! Inc. (“Weee”), an online grocery-delivery service specializing in Chinese and Hispanic ingredients. In February 2023, Weee informed its users that “some customer information” had been leaked in a recent data breach. This putative class action followed, alleging that Weee’s conduct breached (1) New York General Business Law (“GBL”) § 349 and other states’ similar consumer-protection laws, and (2) its implied contract with its customers to “take reasonable measures to safeguard their data.” Dkt. 17 (“Second Amended Complaint” or “SAC”) ¶ 55.

Pending now is Weee’s motion to dismiss plaintiffs’ Second Amended Complaint pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Weee argues that because the information disclosed was “non-sensitive in nature,” plaintiffs have failed to allege an injury in fact sufficient to support Article III standing. Dkt. 20 (“Def. Br.”) at 1. For the reasons that follow, the Court agrees, and thus grants Weee’s motion to dismiss under Rule 12(b)(1).

I. Background

A. Factual Background¹

1. The Parties

Liau created an account with Weee in August 2022 and has purchased goods from Weee since then. SAC ¶ 11. Teng created an account with Weee in October 2021 and purchased goods from Weee “at least twice a month until after the data breach.” *Id.* ¶ 12. Both plaintiffs are New York citizens. *Id.* ¶¶ 11–12.

Weee! Inc. is a Delaware corporation with its principal place of business in California. *Id.* ¶ 13. As an “e-grocer,” Weee does not have brick-and-mortar stores. *See id.* Instead, Weee’s customers use its website and mobile application to place their orders online, and Weee delivers their food to their doorstep. *See id.* Weee pitches itself as the “largest e-grocer specializing in Chinese and Hispanic grocery items in the United States.” *Id.*

2. The Data Breach

On February 6, 2023, a hacker by the name of “IntelBroker” uploaded a subset of Weee’s customers’ personal information to a website on the dark web.² *Id.* ¶ 16. The leak included customers’ names, email addresses, and phone numbers, but not payment data or passwords. *Id.* ¶ 31. Two days later, on February 8, 2023, an online publication focused on cybersecurity, *Bleeping Computer*, published a story about the breach. *Id.* ¶ 16. In that story, Weee confirmed

¹ The Court draws the facts in this decision from the SAC, Dkt. 17, and from documents attached to or incorporated in the SAC. *See DiFolco v. MSNBC Cable LLC*, 622 F.3d 104, 111 (2d Cir. 2010); *Kramer v. Time Warner Inc.*, 937 F.2d 767, 774 (2d Cir. 1991).

² “The [d]ark [w]eb is a general term that describes hidden Internet sites that users cannot access without using special software.” *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 302 n.4 (2d Cir. 2021) (citation omitted). “Not surprisingly, criminals and other malicious actors . . . use the dark web to carry out technology-driven crimes, such as computer hacking, identity theft, credit card fraud, and intellectual property theft.” *Id.* (citation omitted).

that it had “recently bec[o]me aware” of the data breach, which affected customers who “placed an order between July 12, 2021 and July 12, 2022.” Mills Decl., Ex. A at 4.

Plaintiffs’ data was disclosed in the breach. SAC ¶ 16. As to Teng, Weee confirmed as much in an email to him on February 9, 2023, stating that “the exposed information includes [his] name, address, email address, phone number, order number, order amount and order comments,” but that neither his “payment data (credit/debit card detail)” nor his “account password” were disclosed. *Id.* ¶ 31.

3. The Consequences

Plaintiffs allege that they suffered two injuries as a result of the data breach. The first was the “opportunity cost and value of time that [they] have been forced to expend to monitor their financial and bank accounts as a result of the” data breach. *Id.* ¶ 37. In particular, Teng alleges that he was forced to purchase a \$24.99/month subscription to credit-reporting agency Experian’s ID Protection Program, to minimize the “increased risk of identity theft caused by [Weee’s] wrongful conduct.” *Id.* ¶¶ 34–35. The second injury is specific to Teng. He alleges that he has received numerous “spam” telephone calls and text messages due to the leak, which included his phone number. *Id.* ¶ 36.

B. Procedural Background

On February 10, 2023, plaintiffs filed this action, asserting subject matter jurisdiction based on the Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d). Dkt. 1. On May 31, 2023, after Weee moved to dismiss their First Amended Complaint, plaintiffs filed the operative SAC. Dkt. 17.

In the SAC, plaintiffs allege that Weee’s conduct with respect to the leak—and its data-security practices more broadly—breached (1) GBL § 349 and other states’ similar consumer-

protection laws and (2) its implied contract with its customers to “take reasonable measures to safeguard their data.” SAC ¶¶ 51–83. As to their consumer-protection claims, plaintiffs seek to represent “[a]ll persons residing in one of the Consumer Fraud States who registered an account with Weee! e-grocery service at any time from June 21, 2021 through February 6, 2023.” *Id.* ¶ 39.³ As to their implied-contract claim, plaintiffs seek to represent “[a]ll persons residing in the United States who registered an account with Weee! e-grocery service at any time from June 21, 2021 through February 6, 2023.” *Id.* ¶ 38. Plaintiffs seek monetary damages. *See id.* at 18–19.

On June 14, 2023, Weee moved to dismiss the SAC, Dkt. 18, and filed a memorandum of law in support, Dkt. 20 (“Def. Br.”). On June 28, 2023, plaintiffs opposed the motion. Dkt. 21 (“Pl. Br.”). On July 12, 2023, Weee filed a reply. Dkt. 22 (“Def. Reply Br.”).

II. Legal Standard Under Rule 12(b)(1)

In resolving a motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), the Court “must take all facts alleged in the complaint as true and draw all reasonable inferences in favor of plaintiff.” *Nat. Res. Def. Council v. Johnson*, 461 F.3d 164, 171 (2d Cir. 2006). A district court may also consider evidence outside the pleadings, such as affidavits and exhibits. *See Makarova v. United States*, 201 F.3d 110, 113 (2d Cir. 2000); *see also Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 145 (2d Cir. 2011). “A plaintiff asserting

³ The SAC defines the “Consumer Fraud States” as: Arkansas; California; Colorado; Connecticut; Delaware; the District of Columbia; Florida; Hawaii; Idaho; Illinois; Maine; Massachusetts; Michigan; Minnesota; Missouri; Montana; Nebraska; Nevada; New Hampshire; New Jersey; New Mexico; New York; North Dakota; Oklahoma; Oregon; Pennsylvania; Rhode Island; South Dakota; Virginia; Vermont; Washington; West Virginia; and Wisconsin. SAC ¶ 39 n.10.

subject matter jurisdiction has the burden of proving by a preponderance of the evidence that it exists.” *Makarova*, 201 F.3d at 113.

III. Discussion

Weee moves to dismiss the SAC on two grounds. First, under Rule 12(b)(1), it argues that plaintiffs lack standing under *TransUnion LLC v. Ramirez*, 594 U.S. 413 (2021). In the alternative, under Rule 12(b)(6), it argues that the SAC does not state a claim. Because the Court dismisses on the former ground, it does not reach the 12(b)(6) arguments.

A. Applicable Legal Principles as to Constitutional Standing

Article III standing “is the threshold question in every federal case, determining the power of the court to entertain the suit.” *Warth v. Seldin*, 422 U.S. 490, 498 (1975). “[B]ecause standing is necessary to [the Court’s] jurisdiction, [the Court is] obliged to decide the question at the outset.” *Strubel v. Comenity Bank*, 842 F.3d 181, 187–88 (2d Cir. 2016). “If [a] plaintiff[] lack[s] Article III standing, a court has no subject matter jurisdiction to hear [his or her] claim,” and the case must be dismissed without prejudice. *Mahon v. Ticor Title Ins. Co.*, 683 F.3d 59, 62 (2d Cir. 2012) (quotation omitted); *see also Cortlandt St. Recovery Corp. v. Hellas Telecomm’ns S.A.R.L.*, 790 F.3d 411, 416–17 (2d Cir. 2015). A plaintiff must “demonstrate standing for each claim and form of relief sought.” *Cacchillo v. Insmmed, Inc.*, 638 F.3d 401, 404 (2d Cir. 2011) (quoting *Baur v. Veneman*, 352 F.3d 625, 642 n.15 (2d Cir. 2003)). “The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing” each element of constitutional standing. *Id.* (citations omitted).

“[T]he ‘irreducible constitutional minimum’ of standing” requires that the plaintiff have “(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v.*

Robins, 578 U.S. 330, 338 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)). An injury in fact is “an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical.” *Lujan*, 403 U.S. at 560 (cleaned up). Causation requires that the injury be “fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.” *Id.* (cleaned up). Finally, to establish redressability, “it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Id.* at 561 (internal quotation marks omitted).

As the Court explained in *TransUnion*, Article III requires that a “plaintiff’s injury in fact be ‘concrete’—that is, ‘real, and not abstract.’” 594 U.S. at 424 (quoting *Spokeo*, 578 U.S. at 340). To determine whether an alleged injury is sufficiently concrete, a court must assess whether the plaintiff has “identified a close historical or common-law analogue for [his] asserted injury.” *Id.* Although a legislature “may ‘elevate’ harms that ‘exist’ in the real world before [the legislature] recognized them to actionable legal status, [the legislature] may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is.” *Id.* at 426 (quoting *Hagy v. Demers & Adams*, 882 F.3d 616, 622 (6th Cir. 2018)).

B. Application

Plaintiffs contend that they have suffered two injuries-in-fact. The first is the opportunity cost and value of time that [they] have been forced to expend to monitor their financial and bank accounts as a result of the” data breach. *Id.* ¶ 37. The second injury is specific to Teng. He alleges he has received numerous “spam” telephone calls and text messages due to the leak, which included his phone number. *Id.* ¶ 36. The Court addresses each asserted injury in turn.

1. Alleged Monitoring Costs

Plaintiffs allege that they been “forced to” spend time and money “monitor[ing] their financial and bank accounts as a result of the” data breach. *Id.* ¶ 37. Teng, in particular, alleges that he had to subscribe to a \$24.99/month credit-monitoring service—that he would not otherwise have purchased—to minimize the “increased risk of identity theft” attributable to Wee’s security breach. *Id.* ¶¶ 34–35. Even accepting these allegations as true, plaintiffs’ alleged injuries fail to satisfy Article III. That is because plaintiffs cannot “manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 416 (2013).

The Second Circuit recently addressed this very issue—how *TransUnion* applies to a plaintiff who alleges that he was forced to take costly preventive measures after a data breach—in *Bohnak v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276 (2d Cir. 2023). The Circuit explained that a plaintiff may establish concrete harm based on expenses “reasonably incurred” to mitigate “a substantial risk of future identity theft or fraud” as a result of a data breach. *Id.* at 286 (quoting *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021)). For such an expense to be reasonable, however, the plaintiff must show that the risk of misuse is “actual and imminent.” *Id.* at 288. The Circuit set forth “three non-exhaustive factors” that bear on such an inquiry. *Id.* (citing *McMorris*, 995 F.3d at 303). The first “is whether the data was compromised as the result of a targeted attack intended to get” personally identifying information (“PII”). *Id.* (citing *McMorris*, 995 F.3d at 301). The second is whether “some part of the compromised dataset has been misused—even if a plaintiff’s own data has not.” *Id.* (citing *McMorris*, 995 F.3d at 301). The third is “whether the exposed PII is of the type ‘more or

less likely to subject plaintiffs to a perpetual risk of identity theft or fraud once it has been exposed.’” *Id.* (quoting *McMorris*, 995 F.3d at 302).

Here, the first and second factors weigh in plaintiffs’ favor, but ultimately merit little weight so as not to carry the day. As to the first, the data was stolen by a known “threat actor,” IntelBroker. SAC ¶ 2. As to the second, the data was “misused” insofar as the dataset was posted on an online forum. *Id.*; *see also McMorris*, 995 F.3d at 302 (focusing on fact that leaked information was “available for sale on the Dark Web . . . and could therefore be purchased by cybercriminals at any moment”).

But as Judge Furman concluded in a like case, *Cooper v. Bonobos, Inc.*, No. 21 Civ. 854 (JMF), 2022 WL 170622 (S.D.N.Y. Jan. 19, 2022), “that ground crumbles where, as here, the type of data that was exposed is not susceptible to misuse—that is, not ‘sensitive.’” *Id.* at *3. In that situation, the type of “misuse” about which the Second Circuit was concerned—*i.e.*, an “increased risk of identity theft or fraud”—is absent. *Id.*

As the Circuit explained in *Bohnak*:

[T]he dissemination of high-risk information such as [Social Security numbers] especially when accompanied by victims’ names[] makes it more likely that those victims will be subject to future identity theft or fraud. On the other hand, . . . the exposure of data that is publicly available, or that can be rendered useless (like a credit card number unaccompanied by other PII), is less likely to subject plaintiffs to a perpetual risk of identity theft.

79 F.4th at 288 (cleaned up). Here, according to the SAC, the leak at issue was of low-risk data—customers’ names, addresses, and phone numbers, but not their payment data or passwords. SAC ¶ 31.⁴ Such information is often readily available online (and until recently

⁴ In their brief, but not the SAC, plaintiffs suggest that the leak also includes “PID,” which stands for “Personal Identifiable Data.” Pl. Br. at 10. A plaintiff may not amend a complaint “by the briefs in opposition to a motion to dismiss.” *O’Brien v. Nat’l Prop. Analysts Partners*, 719 F. Supp. 222, 229 (S.D.N.Y. 1989). And such an amendment would be unavailing. “PID” is

was generally available in telephone directories). The revelation of “less sensitive data, such as basic publicly available information,” “does not pose the same risk of future identity theft or fraud to plaintiffs if exposed.” *McMorris*, 995 F.3d at 302. And plaintiffs have not plausibly alleged why the leak of the data at issue would causally lead to identity theft. Such a link is required for Teng’s payment for a credit-monitoring service to qualify as a cognizable injury. *Cf. In re SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir. 2017) (“Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.”). “To hold otherwise would allow plaintiffs to string together a lengthy ‘chain of possibilities’ resulting in injury.” *McMorris*, 995 F.3d at 304 (quoting *Clapper*, 568 U.S. at 410).

Plaintiffs have not cited any case where a data breach of relatively quotidian private information of the sort alleged here has been held to support standing based on a plaintiff’s expenditure on preventive measures. To the contrary, the case law has not found an injury in fact where the leak at issue involved information sufficiently less sensitive as realistically not capable of exploitation by malicious actors. *See, e.g., Cooper v. Bonobos, Inc.*, No. 21 Civ. 854 (JMF), 2022 WL 170622, at *4 (S.D.N.Y. Jan. 19, 2022) (no injury in fact where leaked information included customers’ physical “addresses, phone numbers, . . . email addresses, and IP addresses”); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (no injury in fact where leaked information included customers’ “basic contact information, including [their] email address, phone number, or Facebook or Zynga username”); *Kylie S. v. Pearson PLC*, 475

simply shorthand for a *category* of data. *See* Pl. Br. at 10 (describing PID as “including[] but not limited to” data points ranging from a person’s “name” to their “Social Security number”). A general allegation that a leak involved “PID,” without more, lacks the necessary factual detail to fortify plaintiffs’ showing as to the third *Bohnak* factor.

F. Supp. 3d 841, 847–48 (N.D. Ill. 2020) (no injury in fact where leaked information—“students’ names, birthdays, and email addresses”—was “not sensitive enough to materially increase the risk of identity theft”); *see also Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343 (11th Cir. 2021) (in finding no injury in fact, emphasizing that plaintiff did not allege that his Social Security number or date of birth had been compromised in data breach); *SuperValu*, 870 F.3d at 770–71 (similar).

The two cases on which plaintiffs rely do not assist their cause. Each involved sensitive data that *could* more plausibly be used to steal a person’s identity. In *Wallace v. Health Quest Systems, Inc.*, No. 20 Civ. 545 (VB), 2021 WL 1109727 (S.D.N.Y. Mar. 23, 2021), the risk was obvious, given that the leak involved customers’ “names in combination with, dates of birth, Social Security numbers, Medicare Health Insurance Claim Numbers (HICNs), driver’s license numbers, . . . and payment card information.” *Id.* at *2. And in *Rand v. Travelers Indemnity Co.*, 637 F. Supp. 3d 55 (S.D.N.Y. 2022), although Judge Briccetti deemed the injury in fact question “a close call,” he held that the leak of the plaintiff’s “name, address, date of birth, and driver’s license number” warranted some preventive measures, because such information (in particular, the driver’s license number) can readily be “used to file fraudulent unemployment claims, open a new account, take out a loan, or commit income tax refund fraud.” *Id.* at 64, 67. Here, there was no leak of a driver’s license number, but only the name, address, and phone number of the plaintiffs.

The Court thus holds that plaintiffs have not pled an Article III injury in fact based on their claim to have incurred post-leak monitoring costs.

2. Alleged Spam Telephone Calls and Text Messages

Plaintiffs alternatively rely on Teng's allegation that he received "spam" telephone calls and text messages as a result of the leak. SAC ¶ 36. This basis for standing fails on multiple grounds.

First, "[c]ourts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact." *Cooper*, 2022 WL 170622, at *5 (collecting cases); *see also, e.g., Blood v. Labette Cnty. Med. Ctr.*, No. 22 Civ. 4036 (HLT) (KGG), 2022 WL 11745549, at *6 (D. Kan. Oct. 20, 2022) ("[A]lleged inconvenient disruptions (such as spam calls, texts, and emails) do not constitute an injury in fact."); *Jackson v. Loews Hotels, Inc.*, No. 18 Civ. 827 (DMG) (JCX), 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) ("[R]eceiving spam or mass mail does not constitute an injury."); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) ("The receipt of spam by itself . . . does not constitute a sufficient injury entitling [the plaintiff] to compensable relief."). That is because, regrettably, "[s]pam calls, texts, and e-mails have become very common in this digitized world," *McCombs v. Delta Grp. Elecs., Inc.*, No. 22 Civ. 662 (MLG) (KK), 2023 WL 3934666, at *6 (D.N.M. June 9, 2023), and Article III requires an alleged harm that "rise[s] beyond the level [of annoyance] typically experienced by consumers" in their everyday lives, *Gordon v. Virtumundo, Inc.*, No. 06 Civ. 204 (JCC), 2007 WL 145939, at *8 (W.D. Wash. May 15, 2007). The SAC does not allege that the volume or nature of the annoyances experienced by Teng was outsized relative to that reflected in these cases.⁵

⁵ Although plaintiffs do not raise this issue, the decision in *Melito v. Experian Marketing Solutions, Inc.*, 923 F.3d 85 (2d Cir. 2019) is not to the contrary. *Melito* addressed whether plaintiffs suing under the Telephone Consumer Protection Act ("TCPA"), 47 U.S.C. § 227, were required to allege an "injury other than the receipt of the unwanted texts" to establish Article III standing. *Id.* at 88. The Circuit held that such unwanted text messages were alone sufficient.

Second, even were the unwanted annoyances here to reach a level constituting an injury in fact, on the facts alleged, the spam is not “fairly traceable” to Weee’s actions. As Judge Furman explained in *Cooper*, the case of *In re Scientific Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014) [*“In re SAIC”*], is instructive on this point. *See Cooper*, 2022 WL 170622, at *5. There, two plaintiffs alleged they had “received a number of unsolicited calls from telemarketers and scam artists” after their phone numbers and medical records had been revealed in a data breach. 45 F. Supp. 3d at 33. The first plaintiff pled no more. Judge Boasberg found that that plaintiff’s harm could not “plausibly be linked” to the leak, because he “seem[ed] to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls.” *Id.* In contrast, he found, the other plaintiff had “allege[d] a credible link”: not only had her phone number previously been unlisted, but, following the lead, she had received calls for the first time targeting “a specific medical condition listed in her medical records.” *Id.* Teng’s situation is akin to the first plaintiff’s but not the second. The SAC does not connect the spam calls and text messages he has received to the leak, save via the conclusory assertion that “the leak . . . led to” those calls and text messages.

See id. at 92–95. But it did so for reasons specific to the TCPA. “In determining whether an intangible harm . . . constitutes injury in fact,” the Circuit explained, “both history and the judgment of Congress play important roles.” *Id.* at 92–93 (quoting *Spokeo*, 578 U.S. at 340). It was because the “[p]laintiffs allege[d] ‘the very injury the TCPA is intended to prevent’”—the “‘nuisance and privacy invasion’ envisioned by Congress when it enacted” the statute—that plaintiffs’ allegations were sufficient. *Id.* at 93 (cleaned up). Put another way, the plaintiffs did not need to “allege any additional harm *beyond the one Congress has identified.*” *Id.* (emphasis added) (quoting *Spokeo*, 578 U.S. at 342). Here, however, plaintiffs sue under generic state consumer-protection laws (and as to their quasi-contract claims, state common law). Plaintiffs do not and cannot argue that spam text messages are “the very injury” such laws were “intended to prevent.” *Id.* There is thus no basis for the Court to defer to a legislative judgment that the harm alleged here constitutes injury in fact. *Cf., e.g., TransUnion*, 594 U.S. at 425 (emphasizing that “[c]ourts must afford due respect” to legislatures’ views as to whether an alleged intangible harms “qualify as concrete injuries under Article III”).

SAC ¶ 36. The SAC does not, for example, allege that he received *more* spam text messages and calls *after* the leak than before it, or that the spam text messages and calls used information that realistically could be known only via the Weee leak. “[T]he mere allegation” that he has received “spam calls” and “texts . . . does not support standing.” *Cooper*, 2022 WL 170622, at *5; *see also, e.g., Blood*, 2022 WL 11745549, at *6.

The Court accordingly finds that plaintiffs’ alleged injury based on post-leak spam text messages and calls fails to establish Article III standing. The Court therefore dismisses the SAC under Rule 12(b)(1).

C. Leave to Amend

Plaintiffs seek, in the event that the SAC is dismissed, leave to amend. Pl. Br. at 11. Although leave to amend a complaint should be freely given “when justice so requires,” Fed. R. Civ. P. 15(a)(2), it is “within the sound discretion of the district court to grant or deny leave to amend,” *Broidy Cap. Mgmt. LLC v. Benomar*, 944 F.3d 436, 447 (2d Cir. 2019) (internal quotation marks omitted).

The Court denies plaintiffs’ request to replead in this case for a third time. Plaintiffs have had two opportunities to amend their complaint. *See* Dkts. 1, 8. And they have made only a perfunctory request for leave to amend anew in the event of dismissal. They have not identified any concrete amendments or additions, let alone ones that might cure the deficiencies in their claims as to jurisdiction. This supports denial of leave to amend. *See Gregory v. ProNAi Therapeutics Inc.*, 757 F. App’x 35, 39 (2d Cir. 2018) (affirming denial of leave to amend where “plaintiffs sought leave to amend in a footnote at the end of their opposition to defendants’ motion to dismiss” and “included no proposed amendments”); *F5 Capital v. Pappas*, 856 F.3d 61, 89 (2d Cir. 2017) (affirming denial of leave to amend on futility grounds where plaintiff

provided “no clue as to how the complaint’s defects would be cured through an amendment” (internal quotation marks omitted)).

That the dismissal in this case is under Rule 12(b)(1) does not requiring granting leave to amend. *See, e.g., MSP Recovery Claims, Series LLC v. Hereford Ins. Co.*, 66 F.4th 77, 91 (2d Cir. 2023) (affirming denial of leave to amend due to plaintiff’s failure to identify “additional facts or legal theories—either on appeal or to the District Court—they might assert if given leave to amend” that would establish Article III standing (citation omitted)); *Harty v. W. Point Realty, Inc.*, 28 F.4th 435, 445 (2d Cir. 2022) (affirming denial of leave to amend due to plaintiff’s decision to “declin[e] a previous opportunity to amend his complaint” and failure to “request[] an opportunity to amend in the event of a dismissal”); *Meimaris v. Royce*, No. 19-3339, 2021 WL 5170725, at *6 (2d Cir. Nov. 8, 2021) (summary order) (affirming denial of leave to amend as “futile” when plaintiff offered “no indication that there are any additional allegations that could overcome [plaintiff’s] lack of individual standing”).

Given the analysis above, it is difficult to see how any revised claims could overcome the foundational deficiencies in plaintiffs’ theory of Article III standing. “In the absence of any identification of how a further amendment would improve upon the Complaint, leave to amend must be denied as futile.” *In re WorldCom, Inc. Sec. Litig.*, 303 F. Supp. 2d 385, 391 (S.D.N.Y. 2004); *see also, e.g., Panther Partners Inc. v. Ikanos Commc’ns, Inc.*, 347 F. App’x 617, 622 (2d Cir. 2009) (summary order) (“Granting leave to amend is futile if it appears that plaintiff cannot address the deficiencies identified by the court and allege facts sufficient to support the claim.”). “Permitting a new round of repleading in this litigation would therefore . . . further delay already long-delayed litigation and prejudice defendants in their bid for closure.” *Stanley v. City Univ. of N.Y.*, 18 Civ. 4844 (PAE), 2023 WL 2714181, at *26 (S.D.N.Y. Mar. 30, 2023); *see also, e.g.,*

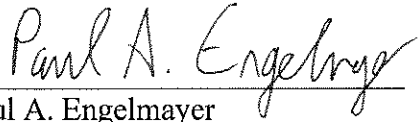
Morency v. NYU Hosps. Ctr., 728 F. App'x 75, 76 (2d Cir. 2018) (“[T]he liberality with which a court grants leave to amend does not impart to litigants the privilege of re-shaping their legal theories endlessly.” (citation omitted)). The Court therefore denies plaintiffs’ request for leave to amend.

For avoidance of doubt, because the dismissal is for lack of subject matter jurisdiction, the dismissal is without prejudice to plaintiffs’ right to pursue—in a separate lawsuit—claims arising from the events above. *See, e.g., MSP Recovery Claims*, 66 F.4th at 91 (although district court denied leave to amend, because “dismissal for lack of jurisdiction is by its nature a dismissal without prejudice,” the dismissal “does not preclude another action on the same claims” (citation omitted)); *Harty*, 28 F.4th at 445 (same); *MAO-MSO Recovery II, LLC v. State Farm Mut. Auto. Ins. Co.*, 935 F.3d 573, 581–82 (7th Cir. 2019) (after dismissal “for lack of jurisdiction without leave to amend,” plaintiffs “may try their luck in state court,” or “if they later believe they can demonstrate that they have suffered an injury in fact after all, . . . they can present these claims against the same defendant in a new federal suit”).

CONCLUSION

For the foregoing reasons, the Court grants Weee’s motion to dismiss under Rule 12(b)(1). The Clerk of Court is respectfully directed to enter judgment, to close this case, and to terminate all pending motions.

SO ORDERED.


 Paul A. Engelmayer
 United States District Judge

Dated: February 22, 2024
 New York, New York